AMENDMENTS TO THE CLAIMS

Claims 1-28 are pending in the instant application. Claims 3-10 and 13-17 have been amended. The Applicant requests reconsideration of the claims in view of the following amendments reflected in the listing of claims.

Listing of claims:

1.   (Original) A method for establishing secure access to a media peripheral in a home via a node in a communication network, the method comprising:

attempting to identify previously acquired security data associated with the media peripheral, and if said security data is not found:

exchanging information associated with the home; and

acquiring security data associated with the media peripheral; and

utilizing said acquired security data associated with the media peripheral to facilitate secure communication between the media peripheral and the communication network.

2.   (Original) The method according to claim 1, wherein said security data is a digital certificate.

3.   (Currently amended) The method according to claim 1, ~~further~~ comprising reading said security data from the media peripheral.

4.   (Currently amended) The method according to claim 1, ~~further~~ comprising transferring said security data to a media exchange server coupled to the communication network.

5.   (Currently amended) The method according to claim 1, ~~further~~ comprising authenticating said security data.

6.   (Currently amended) The method according to claim 1, ~~further~~ comprising, if previously acquired security data associated with the media peripheral is found, acquiring at least one identifier associated with the home.

7.   (Currently amended) The method according to claim 6, ~~further~~ comprising validating said acquired security data prior to communicating over the communication network.

8.   (Currently amended) The method according to claim 7, ~~further~~ comprising registering the media peripheral for subsequent operation.

9.   (Currently amended) The method according to claim 8, ~~further~~ comprising:

establishing at least one user identifier to facilitate communication of the media peripheral over the communication network; and

registering the identifier.

10.   (Currently amended) The method according to claim 8, ~~further~~ comprising distributing security data for said registered media peripheral.

11.   (Original) A method for establishing secure access to a media peripheral via a node in a communication network, the method comprising:

detecting when the media peripheral is communicatively coupled to the node;

acquiring security data associated with the media peripheral; and

utilizing said acquired security data to facilitate secure communication between the media peripheral and the communication network.

12.   (Original) The method according to claim 11, wherein said security data is a digital certificate.

13.   (Currently amended) The method according to claim 11, ~~further~~ comprising reading said security data from the media peripheral.

14.   (Currently amended) The method according to claim 11, ~~further~~ comprising transferring said security data to a media exchange server coupled to the communication network

15.   (Currently amended) The method according to claim 11, ~~further~~ comprising authenticating said security data.

16.   (Currently amended) The method according to claim 11, ~~further~~ comprising registering the media peripheral for subsequent operation.

17.   (Currently amended) The method according to claim 16, ~~further~~ comprising distributing security data for said registered media peripheral.

18.   (Original) A system for establishing secure access to a media peripheral in a home via a node in a communication network, the system comprising:

at least one processor that attempts to identify previously acquired security data associated with the media peripheral, and if said security data is not found:

said processor exchanges information associated with the home; and

said processor acquires security data associated with the media peripheral; and

said processor utilizes said acquired security data associated with the media peripheral to facilitate secure communication between the media peripheral and the communication network.

19. (Original) The system according to claim 18, wherein said security data is a digital certificate.

20. (Original) The system according to claim 18, wherein said at least one processor reads said security data from the media peripheral.

21. (Original) The system according to claim 18, wherein said at least one processor transfers said security data to a media exchange server coupled to the communication network.

22. (Original) The system according to claim 18, wherein said at least one processor authenticates said security data.

23. (Original) The system according to claim 18, wherein said at least one processor acquires at least one identifier associated with the home if previously acquired security data associated with the media peripheral is found.

24. (Original) The system according to claim 23, wherein said at least one processor validates said acquired security data prior to communicating over the communication network.

25. (Original) The system according to claim 24, wherein said at least one processor registers the media peripheral for subsequent operation.

26.   (Original) The system according to claim 25, wherein said at least one processor:

establishes at least one user identifier to facilitate communication of the media peripheral over the communication network; and

registers the identifier.

27.   (Original) The system according to claim 25, wherein said at least one processor distributes security data for said registered media peripheral.

28.   (Original) The system according to claim 18, wherein said at least one processor is at least one of a computer processor, a media peripheral processor, a media exchange system processor and a media processing system processor.